



Protect Against Cyber Threats[®]

Cyber Goblin[™] Field Guide

Recognize the Threats. Strengthen Your Defense

Learn the threats before they learn your organization

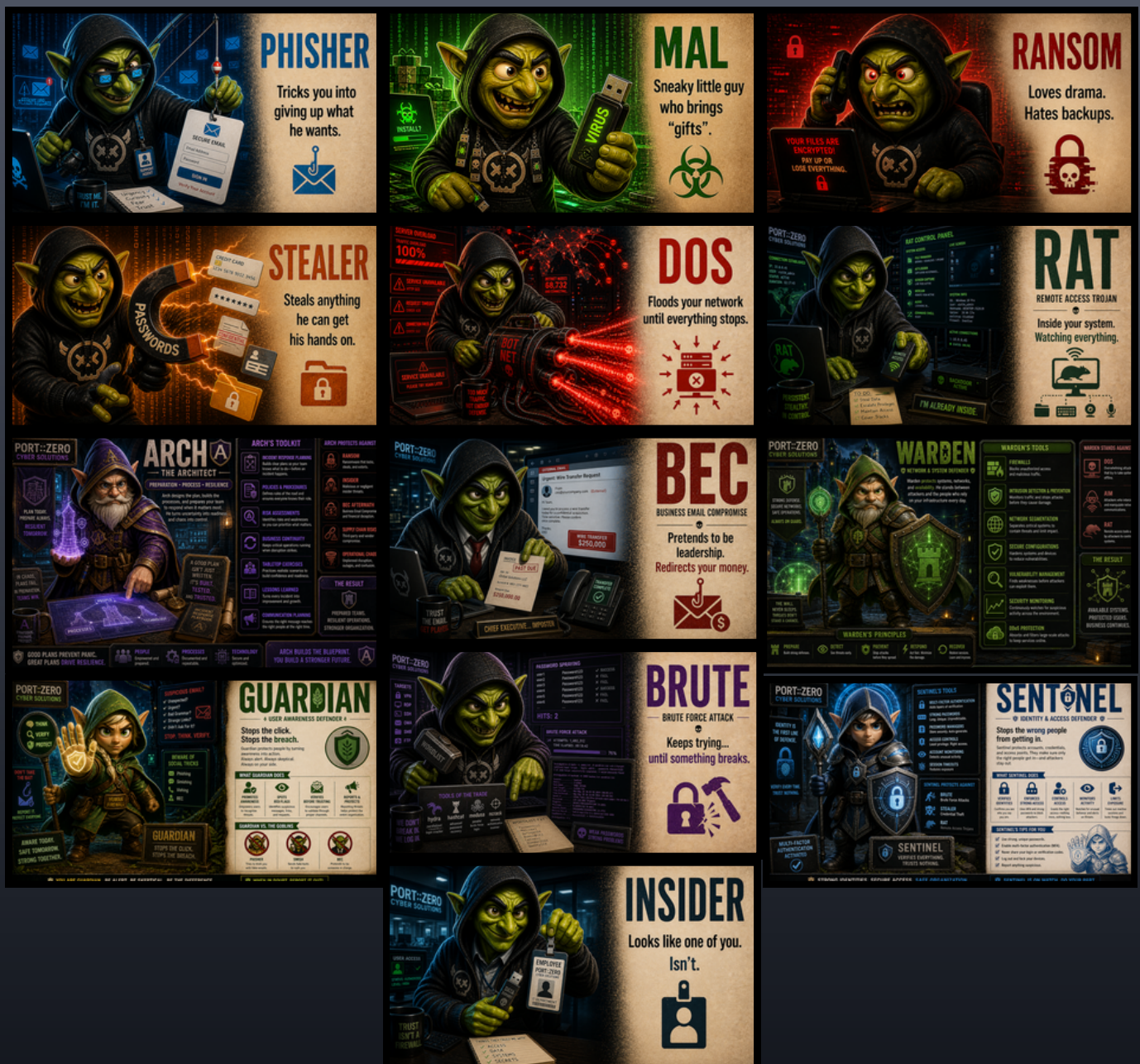


Table of Contents

INTRODUCTION

- What is This Guide?
- How to Use This Guide

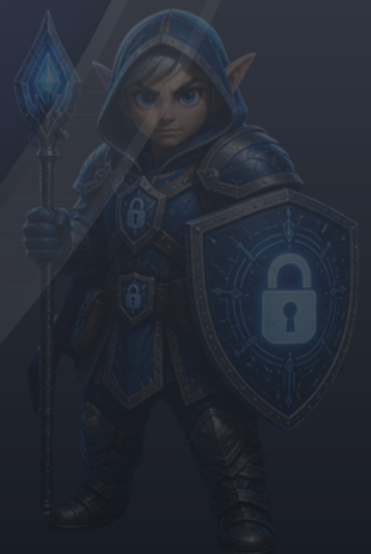
THREATS (THE GOBLINS)

- PHISHER - Email deception and fake links
- SMISH - Text message phishing attacks
- MAL - Malicious software and infected files
- STEALER - Credential and data theft
- BRUTE - Password attacks and automation
- RAT - Remote access and system control
- BEC - Business Email Compromise
- INSIDER - Internal misuse and risk
- RANSOM - Data encryption and extortion
- DOS - Service disruption and downtime



DEFENDERS

- GUARDIAN - Awareness and human defense
- SENTINEL - Identity and access protection
- WARDEN - Monitoring and response
- ARCH - Strategy and resilience



What Is This Guide?

Cyber threats don't always look dangerous.

They often appear as:

- normal emails
- routine requests
- everyday downloads
- familiar login screens

The **Cyber Goblins** represent real-world cyber threats in a simple, visual, and memorable way.

Each goblin highlights how attackers target:

- people
- processes
- technology



By learning to recognize these patterns, you can stop threats before they become incidents.

How to Use This Guide

- Learn each goblin and what they represent
- Recognize common tactics used in real attacks
- Apply simple actions to protect yourself and the organization
- Report anything suspicious quickly

Every attack has a pattern. This guide helps you recognize it.

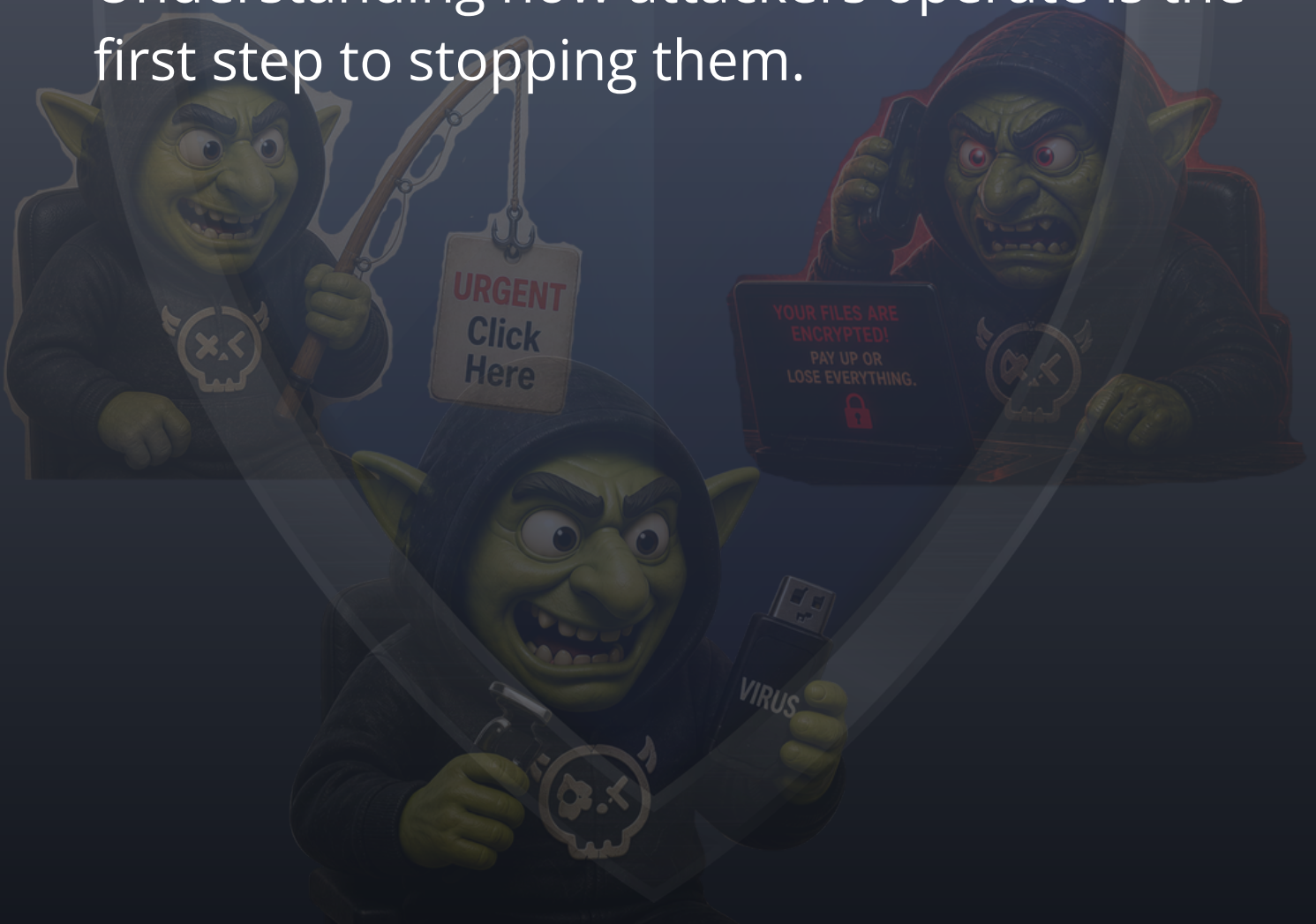
THE GOBLINS

Recognize the threats before they strike.

Cyber threats don't always look dangerous.

They disguise themselves as normal activity: emails, texts, downloads, and requests.

Understanding how attackers operate is the first step to stopping them.



Every attack has a pattern. Learn to see it.

PHISHER

Master of fake links and social engineering tricks.



What It Does

Phisher uses fake emails and links to steal credentials, deliver malware, and trick users into unsafe actions.

Common Signs

- Urgent or threatening language
- Suspicious links or attachments
- Slightly misspelled domains
- Unexpected requests

What To Do

- Don't click on unknown links
- Verify the sender
- Report suspicious messages
- Follow company procedures

Real-World Example

An employee receives an email that appears to be from IT asking them to reset their password immediately. The link leads to a fake login page that captures their credentials.

Quick Defense Rule

If it's urgent, unexpected, or asking for sensitive information, pause and verify before taking action. Protect your accounts with Multi-Factor Authentication (MFA).

SMISH

Text messages that trick you into clicking.



What It Does

SMISH (SMS phishing) uses text messages to trick users into clicking malicious links, sharing sensitive information, or downloading harmful apps. These messages often appear urgent or legitimate.

Common Signs

- Unexpected texts about deliveries, accounts, or payments
- Urgent language ("Act Now", "Your account is locked")
- Shortened or suspicious links
- Messages from unknown or unusual numbers or email addresses

What To Do

- Don't click links in unexpected text messages
- Verify messages through official apps or websites
- Block and report suspicious numbers
- Report the message to your organization

Real-World Example

A user receives a text message stating that their package delivery failed and must be rescheduled. The link leads to a fake site that steals login credentials and payment information.

Quick Defense Rule

If you didn't expect the text, don't trust the link. Verify through official apps or websites.

MAL

Sneaky payloads that infect your system.



What It Does

Mal delivers malicious software through downloads, attachments, and infected devices to steal data, spy on activity, or damage systems.

Common Signs

- Unexpected downloads or installs
- Files from unknown sources
- System slowdowns or strange behavior
- Security warnings or disabled protection

What To Do

- Download only from trusted sources
- Don't open unknown attachments
- Never plug in unknown USB devices
- Report suspicious files or behavior

Real-World Example

An employee plugs in a found USB drive. It installs malware that gives an attacker access to the network and sensitive data.

Quick Defense Rule

Only install or connect what you trust. When in doubt, don't open it, don't plug it in, and report it. Keep systems up to date and protected with endpoint security.

STEALER

Grabs credentials and data wherever it can.



What It Does

Stealer collects credentials, personal data, and sensitive information to gain access to accounts and systems.

Common Signs

- Unrecognized login attempts
- Password reset notifications
- Accounts behaving unexpectedly
- Reused or weak passwords

What To Do

- Use unique passwords for each account
- Enable Multi-Factor Authentication (MFA)
- Use a password manager / passkeys
- Report suspicious account activity

Real-World Example

An employee uses the same password across multiple accounts. After one site is compromised, attackers use those credentials to access company systems.

Quick Defense Rule

If one account is compromised, attackers will try them all. Use unique passwords/passkeys and MFA to stop the chain reaction.

BRUTE

Tries everything until something works.



What It Does

Brute uses automated tools to guess passwords at scale, through brute force, password spraying, and credential stuffing, until it gains access to accounts.

Common Signs

- Multiple failed login attempts
- Account lockouts or throttling alerts
- Login attempts from unusual locations or times
- Repeated attempts against many accounts (password spraying)

What To Do

- Use strong, unique passwords for every account
- Enable Multi-Factor Authentication (MFA)
- Avoid predictable or reused passwords; use passkeys if available
- Report repeated login failures or lockouts

Real-World Example

An attacker runs a password spraying attack using common passwords across many user accounts. A few weak accounts are compromised, giving the attacker a foothold into the network.

Quick Defense Rule

If a password can be guessed, or found on a list, it will be used.
Strong, unique passwords and MFA stop the attack.

RAT

Gives attackers a remote seat at your system.



What It Does

RAT (Remote Access Trojan) installs covert access on a device, allowing attackers to control systems, monitor activity, capture keystrokes, and move laterally across the network.

Common Signs

- Unexpected pop-ups, processes, or services
- Webcam/microphone activating without use
- Unusual outbound connections or data transfers
- System performance issues or unknown programs running

What To Do

- Do not install unknown software or attachments
- Keep systems and applications updated
- Use endpoint protection and allowlisting where available
- Report suspicious behavior immediately

Real-World Example

An employee installs a “free” utility that includes a hidden RAT. The attacker gains remote access, captures credentials, and moves through the network undetected.

Quick Defense Rule

If attackers can control your device, they can control your data. Only install trusted software and report anything unusual immediately.

BEC

Pretends to be leadership. Redirects your money.



What It Does

BEC impersonates executives, vendors, or trusted contacts to trick employees into sending money, changing payment details, or sharing sensitive information, without using malware.

Common Signs

- Urgent payment or wire transfer requests
- Changes to vendor payment instructions
- Requests to bypass normal approval processes
- Slightly altered or lookalike email addresses
- Verify payment requests using known, trusted methods (call-back)
- Follow established approval workflows; no exceptions
- Confirm any changes to vendor banking details
- Report suspicious requests immediately

What To Do

Real-World Example

An employee receives an email that appears to be from the CEO, requesting an urgent wire transfer. The message stresses confidentiality and urgency. The funds are sent, and later it's discovered the email was spoofed and the money is gone.

Quick Defense Rule

No verification, no transaction. Always confirm payment requests and banking changes through a trusted method.

INSIDER

Looks like one of you. Acts like a threat.



What It Does

Insider misuses legitimate access, intentionally or accidentally, to expose data, bypass controls, or disrupt operations. This includes malicious actions, careless behavior, or compromised accounts.

Common Signs

- Accessing data outside normal job duties
- Unusual download or transfer of large files or data
- Sharing credentials or bypassing procedures
- Working in systems at unusual times or locations

What To Do

- Follow least-privilege and access policies
- Never share credentials or accounts
- Report suspicious behavior or access immediately
- Ask before using unauthorized tools or services

Real-World Example

An employee uploads sensitive files to a personal cloud account to work from home. The account is later compromised, exposing company data to attackers.

Quick Defense Rule

Trusted access requires accountability. Follow policy, protect credentials, and report anything that doesn't look right. Insider risk is often careless, not malicious.

RANSOM

Locks your data and demands payment.



What It Does

Ransom encrypts files and systems, preventing access until a payment is made. It can spread across networks quickly, disrupting operations and causing significant downtime.

Common Signs

- Files suddenly become inaccessible or locked
- Ransom note appears on screen
- Systems slow down or lock up
- Unusual file extensions

What To Do

- Disconnect affected systems immediately
- Report the incident to IT or security
- Do not attempt to pay or negotiate without leadership and security guidance
- Follow your organization's incident response plan

Real-World Example

An employee opens a malicious attachment that installs ransomware. Within minutes, shared drives become encrypted, and the organization loses access to critical systems and data.

Quick Defense Rule

If your data isn't backed up, it's already at risk. Regular, tested backups are your best defense against ransomware.

DOS

Overwhelms systems until they stop responding.



What It Does

DOS (Denial of Service) overwhelms a system, website, or network with excessive traffic or requests, preventing legitimate users from accessing services. Large-scale attacks (DDoS) use many sources at once to amplify the impact.

Common Signs

- Website or application becomes slow or unavailable
- Sudden spikes in traffic or requests
- Users can't log in or access services
- Alerts from monitoring tools about service outages

What To Do

- Report outages or unusual slowdowns immediately
- Follow incident response and communication procedures
- Avoid making unapproved changes during the outage
- Direct users to approved status pages or channels

Real-World Example

A public-facing website is flooded with traffic from thousands of sources, causing it to crash. Customers can't access services, and the organization loses revenue and trust during the outage.

Quick Defense Rule

If your services go down, your business stops. Preparation and response determine how fast you recover; availability is key to business continuity.

THE DEFENDERS

Strengthen your defenses. Protect what matters.

Security isn't built on a single tool; it's built in layers.

Awareness, identity protection, monitoring, and strategy work together to prevent threats from becoming incidents.

When these defenses are aligned, organizations become resilient.



Defense is a system, not a single solution.

GUARDIAN

Recognizes the threat before it succeeds.



What It Does

Guardian represents trained, aware users who recognize suspicious activity, question unexpected requests, and take the right action to stop threats before they become incidents.

Core Capabilities

- Identifies phishing, smishing, and suspicious behavior
- Verifies requests before taking action
- Follows security policies and procedures
- Reports threats quickly and accurately

Tools & Practices

- Security awareness training
- Phishing and smishing recognition skills
- Clear reporting processes ("Report Phish" button)
- A culture that encourages speaking up

Real-World Example

An employee receives a message requesting urgent payment. Instead of acting immediately, they verify the request through a trusted method and report it, preventing a BEC incident.

Quick Defense Rule

Awareness is your first line of defense. When something feels off, pause, verify, and report.

SENTINEL

Verifies identity before granting access.

What It Does

Sentinel represents identity and access controls that verify users before granting access. It protects accounts with Multi-Factor Authentication (MFA), passkeys, and strong authentication, stopping unauthorized logins even if passwords are compromised.



Core Capabilities

- Enforces Multi-Factor Authentication
- Uses passkeys and phishing-resistant login methods
- Applies access controls and least privilege
- Monitors and flags suspicious login activity

Tools & Practices

- MFA (app-based, hardware tokens, etc.)
- Passkeys (phishing-resistant authentication)
- Password managers for strong, unique credentials
- Account monitoring, alerts, and session timeouts

Real-World Example

An attacker obtains a user's password from a data breach. When they attempt to log in, MFA blocks access. The user receives a login alert and reports the attempt, preventing account takeover.

Quick Defense Rule

Passwords get stolen, and verification stops the attack. Use MFA or passkeys on every account.

WARDEN

Sees the threat, and responds before it spreads.



What It Does

Warden represents monitoring and detection systems that collect logs, identify suspicious activity, and trigger alerts, enabling rapid response to contain and stop threats.

Core Capabilities

- Centralized logging and visibility across systems
- Detects anomalies and suspicious behavior
- Generates alerts for potential incidents
- Enables rapid containment & response

Tools & Practices

- SIEM (Security Information and Event Management)
- Endpoint Detection & Response (EDR/XDR)
- Log collection and correlation
- Alerting, playbooks, and incident response procedures

Real-World Example

Unusual login activity from a foreign location triggers an alert in the SIEM. The security team investigates, isolates the account, and prevents further unauthorized access.

Quick Defense Rule

You can't stop what you can't see. Monitoring and alerts turn activity into action.

ARCH

Designs security. Builds resilience. Protects the future.



What It Does

Arch represents security architecture and strategy, designing systems, processes, and policies that reduce risk, ensure resilience, and enable the organization to prevent, withstand, and recover from cyber incidents.

Core Capabilities

- Designs secure systems and architectures
- Identifies and prioritizes risk
- Plans for resiliency and recovery
- Establishes governance, policies, and standards

Tools & Practices

- Security architecture frameworks (NIST, CIS, Zero Trust)
- Risk assessments and threat modeling
- Business Continuity & Disaster Recovery (BC/DR) planning
- Policies, standards, and governance programs

Real-World Example

An organization designs its environment with backups, segmentation, and incident response plans in place. When ransomware strikes, systems are restored quickly with minimal impact to operations.

Quick Defense Rule

Strong security isn't luck, it's architecture. Plan today. Protect tomorrow.

PROTECT AGAINST CYBER THREATS

Cyber threats are constantly evolving, but so are the defenses that stop them.

Organizations that succeed don't rely on luck; they build security intentionally.

They build awareness, enforce strong controls, monitor activity, and design for resilience.

The Cyber Goblin Framework™

The Cyber Goblin Framework is a structured approach to cybersecurity awareness and defense, combining real-world threat recognition with practical protection strategies across people, processes, and technology.

CORE Pillars

- **Awareness** - Train your people (Guardian)
- **Identity Protection** - Secure access (Sentinel)
- **Monitoring & Response** - Detect and act (Warden)
- **Strategy & Design** - Build resilience (Arch)

Ready to strengthen your organization?

- Cybersecurity Awareness Training
- Incident Response Planning
- Security Assessments

PORT::ZERO Cyber Solutions

 portzerocyber.com

 rick@portzerocyber.com

 (877) 317-4422

Strong security isn't luck, it's built.